Volume 3, Issue 5 September 2017

Homeland Security

CFATS Quarterly

Chemical Facility Anti-Terrorism Standards

Compliance Close-Up: Getting to Know Your CSAT 2.0 SVA/SSP

Last fall, DHS released the Chemical Security Assessment Tool (CSAT 2.0) which streamlined the Chemical Facility Anti-Terrorism Standards (CFATS) online processes, including the Security Vulnerability Assessment (SVA)/Site Security Plan (SSP) survey. The SVA/SSP contains clarifications and new questions necessary to implement the enhanced tiering methodology while still drastically reducing the number of overall questions. To ensure a smooth and efficient transition, the majority of the information that facilities have previously submitted is pre-populated into the new survey.

However, when you revise the SVA/SSP in CSAT 2.0 for the first time, there are several new questions you will need to answer. On the SVA, these questions include reviewing the currently tiered Chemical of Interest (COI), voluntarily adding non-tiered COI, and identifying COI use, critical assets, and overall security measures and vulnerabilities.

On the SSP, new questions that facilities will need to address include:

Q3.10.050 Personnel Presence
Q3.10.400 through Q3.10.420 Inventory Controls
Q3.40.400 through Q3.40.430 Cyber Control and Business Systems
Q3.50.320 Personnel Surety, Types of Affected Individuals
Q3.50.710 Recordkeeping Affirmation*
*This question alone replaces 15 questions in the previous survey!

The improved SVA allows facilities to define critical assets, which allow for streamlined responses in the section of the SSP where facilities are asked to select whether a certain detection and delay measure applies to the perimeter and/or critical assets. Facilities should revisit the following SSP questions to correctly identify the location(s) to which each security measure applies:

Q3.10.070 Mobile Patrols
Q3.10.120 Intrusion Detection Systems
Q3.10.180 through Q3.10.230 Intrusion Detection Sensors
Q3.10.290 and Q3.10.310 Closed Circuit Television
Q3.20.030 through Q3.20.160 Perimeter Security
Q3.20.430 and Q3.20.440 Access Control Systems
Q3.20.560 Anti-Vehicle Measures

Tier 1 and Tier 2 facilities will see questions that address Risk-Based Performance Standard (RBPS) 12(iv), screening for terrorist ties. Questions Q3.50.330 through Q3.50.550 allow facilities to identify the option(s) chosen and measure(s) used to implement those options for compliance with RBPS 12(iv).

Additionally, the Department's Personnel Surety Program (PSP) is going to be integrated into the CSAT Portal in order to provide better functionality for the end user.

Don't forget to review your planned measures and ensure they transferred or updated as appropriate. Questions about the compliance process? Contact the Help Desk at CSAT@hq.dhs.gov.

CFATS Update

As of September 1, CFATS covers **3,478** facilities, and DHS has completed more than **2,700** total compliance inspections. Stakeholders can expect to see the number of facilities evolve as additional facilities submit the updated Top-Screen and receive new tiering determinations. Since launching the streamlined CSAT 2.0 surveys and enhanced tiering methodology last fall, DHS has received more than **25,000** CSAT 2.0 Top-Screens. We continue to issue tiering determination letters as Top-Screens are received and processed. As always, we remain ready to address your questions and concerns. If you have questions about CSAT 2.0 or compliance, contact the Help Desk at 866-323-2957 or CSAT@hq.dhs.gov.

Chiefs of Regulatory Compliance

We're happy to announce that we have hired Chiefs of Regulatory Compliance (CRCs) for almost all of our Regional Offices. CRCs will serve as the lead DHS representatives administering the CFATS regulation and serving as advisors to the Office of Infrastructure Protection Regional Directors.

In addition to managing CFATS regional operations, CRCs will lead our regional efforts to coordinate with other federal, state, and local representatives and spearhead regional CFATS-related outreach and engagement.

Region 1 (VT, RI, ME, NH, CT, MA)
Charles Colley charles.colley@hq.dhs.gov

Region 2 (VI, PR, NJ, NY)
John Dean john.dean@hq.dhs.gov

Region 3 (DC, DE, WV, MD, VA, PA)
Don Keen donald.keen@hq.dhs.gov

Region 4 (MS, SC, AL, KY, FL, NC, TN, GA)
Cheryl Louck cheryl.louck@hq.dhs.gov

Region 5 (MN, WI, IN, MI, IL, OH)
Kathy Young kathryn.young@hq.dhs.gov

Region 6 (NM, OK, LA, AR, TX)
Steve Shedd steven.shedd@hq.dhs.gov

Region 7 (NE, KS, IA, MO)
Dave Martak* david.martak@hq.dhs.gov

Region 8 (WY, ND, SD, MT, UT, CO)
Jim Williams james.williams@hq.dhs.gov

Region 9 (MP, GU, HI, NV, AZ, CA)
Marcie Stone marcie.stone@hq.dhs.gov

Region 10 (AK, ID, OR, WA)
Marc Glasser marc.glasser@hq.dhs.gov

*Acting

Region 10 CRC Marc Glasser

Are Your Physical Security Measures Fit for the Cyber World?

Protecting against cyber sabotage is an essential component in managing overall risk for a facility. Cybersecurity and physical security are becoming even more interconnected—but are your physical security measures themselves protected?

Many physical security solutions now incorporate a digital element that needs securing like any other cyber system. For example, consider the security cameras used to monitor points of entry and assets at a facility. Some security cameras can be connected to each other and to a monitoring station utilizing Wi-Fi or an Ethernet connection into the existing network. These features allow for easier set up and installation as new communication wiring does not need to be run for each individual camera. But along with this convenience comes a potential exploit: if the cameras don't include security software, or if that software is not maintained, malicious actors could utilize these vulnerabilities to disable the camera, install malware, or even intercept or spoof the video stream.

Any device that can connect to a network becomes part of the "Internet of Things" (IoT), and is potentially susceptible to exploitation by an outside party. Some other examples of devices that might have network connections are multifunction printers, inventory scanners, or process control systems with web-based management.

Best practices for securing devices that can be connected to a network (regardless of whether the feature is being used or not) include disabling default connections and default settings, changing default usernames and passwords, checking for and applying firmware and software updates as soon as they are available, and following a policy of least privilege access. For an increased level of security, place the devices in an isolated network and administer access to that network segment accordingly.

Just because a device is not utilized for a cyber purpose does not always mean that it is not susceptible to a cyber-attack.

Resources

Outreach: To request a CFATS presentation or a Compliance Assistance Visit, submit a request through www.dhs.gov/critical-infrastructure-chemical-security, or CFATS@hq.dhs.gov.

CFATS Help Desk: Hours of Operation are Mon. - Fri., 8:30 AM to 5:00 PM (EST). Contact 866-323-2957 or CSAT@hq.dhs.gov.

Website: For Frequently Asked Questions (FAQs), Chemical-terrorism Vulnerability Information (CVI) training, and other CFATS-related information, visit www.dhs.gov/chemicalsecurity.

Inspectors: Email CFATS@hq.dhs.gov to receive the contact information of the inspector for your area.

2017 Chemical Sector Security Summit

In July, more than 500 chemical stakeholders attended the 11th annual Chemical Sector Security Summit to discuss risks to the chemical industry, disaster planning, and the resources DHS offers to mitigate the threat of a terrorist attack using industrial chemicals.

The Summit is the result of a private-public partnership between the NPPD Office of Infrastructure Protection and the Chemical Sector Coordinating Council, which cosponsored the event.

This year, the Summit was held in Texas, one of the largest concentration of chemical facilities in the nation, and home to more than 250 high-risk CFATS facilities.

Sessions provided participants with the opportunity to engage in face-to-face discussions, and share best practices and lessons learned. Presentations included cyber and physical security, updates on the CFATS program, active shooter preparedness, a live hacking demo on a facility, and security roles during a disaster.

"The Chem Summit epitomizes the work we are doing here at the Office of Infrastructure Protection to bring together stakeholders from all types of backgrounds—public, private, regulatory, and voluntary—to work together to continue to enhance the security and resilience of our nation's chemical infrastructure," said Dave Wulf, Acting Deputy Assistant Secretary for IP.

The Summit was covered in local and international media, including an op-ed in the Houston Chronicle and a feature by Voice of America.

Top: Kirsten Meskill of BASF/Bottom: Acting Deputy Assistant Secretary for IP Dave Wulf ringing a model of the Chemical Security Bell.

Featured CFATS Materials

DHS is committed to providing our stakeholders information on how to implement the CFATS program. Since the last issue of the CFATS quarterly, we have published several new fact sheets and flyers, some of which were the result of feedback from stakeholders. If you have ideas for future products, please contact us at CFATS@hq.dhs.gov.

Records Fact Sheet and Sample Records: We have created a fact sheet about Risk-Based Performance Standard (RBPS) 18—Records, which is accompanied by sample records that can be downloaded and used by facilities if they wish. Facilities are free to use their own records format that meet the RBPS—these are voluntary tools that we think might be of help based on some of the questions we've received from facilities. Find out more about RBPS 18 and download the samples at: www.dhs.gov/cfats-rbps-18-records.

Flyer on Reporting CFATS Violations: In the Department's experience, the majority of regulated facilities have worked to come into compliance with the CFATS program by fulfilling their obligation to report holdings of Chemicals of Interest (COI) and, if deemed high-risk, to implement security measures to protect their COI from use in a terrorist attack. We have published a printable flyer on CFATS violations—what constitutes a violation and how to report one. The flyer is available for download at www.dhs.gov/report-cfats-violation.

Penalty Policy and Fact Sheet: As you know, enforcement of compliance with the CFATS program is important in ensuring our nation's high-risk chemical facilities continue to have the necessary anti-terrorism safeguards in place. While we take every opportunity to discuss options and provide the necessary support, there are times when we need to use other avenues to ensure compliance. The CFATS Penalty Policy and Fact Sheet outline the policies and procedures that DHS follows to issue an order assessing a civil penalty to a chemical facility found to be in violation of the *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014*. The policy and related fact sheet can be found at www.dhs.gov/cfats-penalty-policy.

Flyer for Shipments of COI: In response to stakeholder feedback, the Department has created a flyer that facilities can choose to use when shipping or transferring COI from their facilities. Facilities are not required to share this flyer, but may choose to use it to assist their customers and partners in understanding their regulatory obligations. The flyer is available for download at www.dhs.gov/publication/receiving-coi-flyer. It is suitable for electronic or printed use, and can be reproduced and distributed as needed.